IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,)
)
Plaintiffs,)
)
v.)
) Case No. 1:96CV 01285
) (Judge Lamberth)
GALE A. NORTON, Secretary of the Interior, et al.,)
)
Defendants.)
)

INTERIOR DEFENDANTS OPPOSITION TO PLAINTIFFS' CONSOLIDATED MOTION FOR A TEMPORARY RESTRAINING ORDER AND MOTION FOR A PRELIMINARY INJUNCTION TO ENSURE THE PROTECTION OF INDIVIDUAL INDIAN TRUST DATA

Pursuant to Rule 65 of the Federal Rules of Civil Procedure and Local Civil Rule 65.1, Interior Defendants respectfully submit the following opposition to plaintiffs' Consolidated Motion for a Temporary Restraining Order and Motion for a Preliminary Injunction to Ensure the Protection of Individual Indian Trust Data ("Plaintiffs' Motion").

I. Plaintiffs' Motion is Without Merit and Should Be Denied Because Plaintiffs Cannot Establish Any of the Elements Required for Issuance of a Temporary Restraining. Order

In considering whether to grant an application for a temporary restraining order or a preliminary injunction, this Court must examine (1) whether there is a substantial likelihood that the plaintiff would succeed on the merits, (2) whether the plaintiff would suffer irreparable injury if the injunctive relief is denied, (3) whether the granting of injunctive relief would substantially injure the other party, and (4) whether the public interest would be served by the granting of the injunctive relief. E.g., Davenport v. International Brotherhood of Teamsters, AFL-CIO, 166 F.3d

356,360-61 (D.C. Cir. 1999) (citing Serono Laboratories, Inc. v. Shalala, 158 F.3d 1313, 1317-18 (D.C. Cir. 1998)); Kudjodi v. Wells Fargo Bank, 181 F. Supp. 2d 1, 2 note 2 (D.D.C. 2001).

In their Motion, plaintiffs seek an order directing as follows:

- ". . . that Interior defendants immediately shall disconnect from the Internet all information technology systems which house or provide access to individual Indian trust data until such time as the Special Master has determined that all individual Indian trust data is properly secured . . ." and
- ". . . that Interior defendants immediately shall disconnect from the Internet all computers within the custody and control of the Department of the Interior, its employees and contractors, that house or provide access to individual Indian trust data until such time as the Special Master has determined that all individual Indian trust data is properly secured . . . ."

Plaintiffs' Motion at 9-10 (proposed temporary restraining order).

A. Plaintiffs Have Not Established a Substantial Likelihood of Success of the Merits

It is of critical importance for this Court to appreciate that the issue which has arisen between the Interior Department and the Special Master pertains to the testing under the draft rules of engagement described below. Contrary to plaintiffs' assertions, the issue between the Interior Department and the Special Master does not pertain to the procedures for verifying reconnection proposals under the Consent Order entered December 17, 2001 (the "Consent Order").

Pursuant to the Consent Order, the Interior Defendants have submitted to the Special

Master proposals to reconnect various information technology systems that had previously been disconnected from the Internet following the Court's December 5,2001 Temporary Restraining Order. Moreover, the Consent Order provides that the Special Master has authority to "verify compliance with the Consent Order." Consent Order at 7.[1]

With the exception of special procedures applicable to limited reconnections for testing and the provision of certain necessary services, Consent Order at 6-7, the Consent Order generally provides that Interior Defendants may reconnect systems following notice to the Special Master if such systems (a) do not house or provide access to individual Indian trust data or (b) house or provide access to individual Indian trust data, provided adequate security exists. Consent Order at 5-6, 7. Where the systems house or provide access to individual Indian trust data, the Consent Order provides, "The Special Master shall review the plan [for reconnection] and perform any inquiries he deems necessary to determine if it provides adequate security for individual Indian trust data." Consent Order at 7.

Finally, the Consent Order expressly provides "that the Special Master shall verify compliance with this Consent Order and may conduct interviews with Interior personnel or contractors or conduct site visits wherever information technology systems or individual Indian trust data is housed or accessed." Consent Order at 7. Thus, by its terms, the Consent Order

- established a mechanism for reconnecting Interior Department systems to the

[1] We note that only the plaintiffs – not the Special Master – have raised with the Court questions regarding the adequacy of the security of the Interior Department's information technology systems. The Interior Department has submitted to the Special Master numerous reconnection proposals – approved by the Special Master – since the issuance of the Consent Order, as is confirmed in the Special Master's reports to the Court. If the plaintiffs have concerns about the security of these systems, then they should raise them initially with the Special Master.

Internet, primarily through proposals submitted to the Special Master that showed the systems either (i) did not house or provide access to individual Indian trust data or (ii) provided "adequate security" for individual Indian trust data.

- provided the specific authority for the Special Master to verify the information set forth in the proposals.

Contrary to plaintiffs' assertion, Plaintiffs' Motion at ***6,*** the Consent Order did not establish a continuing right for the Special Master to access any Interior Department information technology system at any time, nor did it provide authorization for the Special Master to conduct intrusive and potentially destructive "penetration" and "exploitation" testing. This is critical because 18 U.S.C. § 1030 provides that it is a felony for a person to seek to gain unauthorized access to information housed on Government computer systems. For example, subsection 1030(a)(2)(B) proscribes a person from "intentionally acessess[ing] a computer without authorization or [in excess of] authorized access" and thereby obtaining "information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). See also 18 U.S.C. § 1030(a)(3) (proscribing access to "any nonpublic computer of a department or agency of the United States" and thereby affecting use of the computer "by or for the Government of the United States"); 18 U.S.C. § 1030(a)(5)(B)((iv)-(v) (proscribing "transmission of a program, information, code, or command" that causes or would have caused "a threat to public health or safety" or "damage affecting a computer system used . . . in the administration of justice, national defense, or national security").

Given the issue of whether 18 U.S.C. § 1030 would have application beyond the Consent Order, beginning in the latter half of 2002, the Interior Department and the Special Master undertook to develop a protocol – later known **as** the "draft rules of engagement" – to allow such testing by the Special Master. E.g., Exhibit A (September 2002 Report of Special Master at **2** (Oct. 4,2002) ("In addition, [the Special Master's expert] has been working with [the Interior Department's expert] to develop protocols to safely monitor the security of Interior's computer's systems.")); Exhibit B (January 2003 Report of Special Master at **2** (Feb. 3,2003) ("The Special Master and Interior have agreed, in principle, to 'rules of engagement' that would govern [the Special Master's expert's] scans of Interior computer systems. Once a final copy is promulgated, it will be distributed to the Court and parties.")). See also Exhibit C (letter to Special Master from J. Warshawsky (Nov. 22,2002) (transmitting draft rules of engagement)).

The draft rules of engagement further defined various levels of testing, referred to as Phases One, Two, Three, and Four. E.g., Exhibit C (first page of letter, pages 3-5 of Interior Department draft, and first page of Usinternetworking attachment). **As** the description of these phases confirm, the types of testing under the draft rules of engagement are increasingly intrusive and potentially destructive. See Exhibit C (first page of Usinternetworking attachment describing "Open-source information gathering," "Network Asset Discovery," "Vulnerability/Penetration Testing," and "Exploitation Limits Testing"). The draft rules of engagement further provided for limited notice to Government officials – known as "Trusted Points-of-Contact" – the scope of which depended upon the type of testing to be conducted.

It is of critical importance for this Court to appreciate that the issue which has arisen between the Interior Department and the Special Master pertains to the testing under the draft rules of engagement; it does not pertain to the procedures for verifying reconnection proposals under the Consent Order. Plaintiffs' Motion does not establish a likelihood of success, substantial or otherwise, because they confuse the consent required for access under the draft rules of engagement with the Special Master's duty to verify proposals to reconnect under the Consent Order.[2] The testing referred to in the correspondence attached to Plaintiffs' Motion was with respect to the draft rules of engagement, not the Consent Order.

Therefore, Plaintiffs' Motion fails to establish the first element for the granting of a temporary restraining order. The Interior Department has not violated the Consent Order, nor has it withdrawn its consent under the Consent Order. The Interior Defendants have, however, lost confidence in the draft rules of engagement because the Special Master will not accept the representations of the Trusted Points-of-Contact. Accordingly, the Interior Department notified the Special Master that the unresolved differences described in the correspondence attached to Plaintiffs' Motion prevents further testing under the now-inadequate draft rules of engagement.

B. Plaintiffs' Motion Does Not Establish the Potential for "Irreparable Harm" if Their Motion is Not Granted

Plaintiffs' Motion provides no specific information to support the assertion that they will suffer irreparable harm if a temporary restraining order is not granted. To the extent plaintiffs provide any specific assertions, they are with respect to two servers of the Office of Surface Mining, neither of which houses or provides access to individual Indian trust data, even applying

[2] To the extent plaintiffs seek to rely upon the specific facts surrounding the disconnected OSM server, the plaintiffs have wholly failed to adduce any evidence to support the unfounded assertion that a Trusted Point-of-Contact was involved in the disconnection of the server. Plaintiffs' Motion at 2-3. Indeed, the only evidence – discussed in the letters attached to Plaintiffs' Motion and attested to on June 5, 2003, by Mr. Cason during the Phase 1.5 trial – indiciates that the cable's disconnection was coincidental and benign.

the broadest reasonable definition to that term.[3]

C. The Granting of Plaintiffs' Motion Would Substantially Harm Interior Defendants

Unlike most scenarios in which a temporary restraining order is sought, this Court already has the benefit of knowing the impact of the December 5,2001 temporary restraining order. The Court is well-aware of the cost to both IIM beneficiaries and the Government – financial and otherwise – resulting from the disconnection of the Interior Department's systems in December 2001. Plaintiffs' Motion seeks to undo the efforts since December 17, 2001, which resulting in the reconnection of many Interior Department systems. See June 19,2003 letter from Special Master to Ms. Spooner (next-to-last letter among plaintiffs' exhibits) (referring to efforts "to reconnect 95% of Interior's systems within one year of the [December 5,2001 Order]"). For obvious reasons, Plaintiffs' Motion does not address the harm to Interior Defendants.

D. The Granting of Plaintiffs' Motion is Not in the Public's Interest

For many of the same reasons described immediately above, the granting of the Plaintiffs' Motion would harm the public, not serve the public's interest. **As** the Court is well-aware, the disconnection of the Interior Department's information technology systems negatively impacted a vast array of individuals and entities – including members of the plaintiffs' class. Moreover, as the Court is aware from the events subsequent to December 5,2001, Interior Defendants' information technology systems impact the National Critical Infrastructure Systems and are

[3] We note that the Office of Surface Mining systems were reconnected pursuant to the Consent Order's provision applicable to systems that do not house or provide access to individual Indian trust data. Exhibits D (transmittal letter to Special Master for December 21, 2001 reconnection proposal) and E (letter to Special Master dated January 22,2002, confirming authorization to reconnect).

involved in matters affecting public health, safety, and national security. Again, it is clear that the granting of Plaintiffs' Motion is not in the public's interest, and plaintiffs have made no serious attempt to argue to the contrary.

Conclusion

Plaintiffs' Motion confuses verification of reconnection proposals under the Consent Order with the continuing testing contemplated by the draft rules of engagement being negotiated between the Special Master and the Interior Defendants. Moreover, Plaintiffs' Motion fails to establish any of the four elements necessary for the granting of a temporary restraining order. For the foregoing reasons, we respectfully request that the Court deny Plaintiffs' Motion.

Respectfully submitted,

ROBERT McCALLUM, JR.
Assistant Attorney General

STUART E. SCHIFFER
Deputy Assistant Attorney General

J. CHRISTOPHER KOHN
Director

SANDRA P. SPOONER (D.C. Bar No. 261495)
Deputy Director
JOHN T. STEMPLEWICZ
Senior Trial Attorney
JOHN WARSHAWSKY (D.C. Bar No. 417170)
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875, Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 514-7194

June 27,2003

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,)
)
Plaintiffs,)
)
v.) Case No. 1:96CV01285
) (Judge Lamberth)
GALE A. NORTON, Secretary of the Interior, et al.,)
)
Defendants.)
)

ORDER

This matter comes before the Court on Plaintiffs' Consolidated Motion for a Temporary Restraining Order and Motion for a Preliminary Injunction to Ensure the Protection of Individual Indian Trust Data. After considering that motion, Interior Defendants' response thereto, and the record of the case, the Court finds that the plaintiffs' motion should be, and hereby is, DENIED.

SO ORDERED this ___ day of _____________, **2003.**

____
ROYCE C. LAMBERTH
United States District Judge

cc:

Sandra P. Spooner
John T. Stemplewicz
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Fax (202) 514-9163

Mark Kester Brown, Esq.
Dennis M. Gingold, Esq.
607 - 14th Street, NW
Box **6**
Washington, DC 20005
Fax (202) 318-2372

Keith Harper, Esq.
Native American Rights Fund
1712 N Street, NW
Washington, D.C. 20036-2976
Fax (202) 822-0068

Elliott Levitas, **Esq.**
1100 Peachtree Street, Suite 2800
Atlanta, GA 30309-4530

Alan L. Balaran, Esq.
Special Master
1717 Pennsylvania Avenue, N.W.
13th Floor
Washington, D.C. 20006
(202) 986-8477

Earl Old Person ***(Prose)***
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
(406) 338-7530

LAW OFFICE
ALAN L. BALARAN,P.L.L.C.
ADMITTED IN DC AND MD

1717 PENNSYLVANIA AVE., N.W.
TWELFTH FLOOR
WASHINGTON, D.C 20006
TELEPHONE (202) 466-5010
FAX (202) 986-8477
E-MAIL abalann@nok.com

October 4, 2002

Honorable Royce C. Lamberth
United States District Court
for the District of Columbia
333 Constitution Ave., N.W.
Washington, D.C. 20001

RE: <u>Cobell et al. v. Norton et al.</u>, **C.A. No. 96-1285**
September 2002 Report of Special Master

Dear Judge Lamberth:

In accordance with this Court's Order dated February 24, 1999 appointing me as Special Master, I am submitting my September 2002 monthly report. The Court has graciously granted my request for an extension of time in which to file this Report.

I. <u>Contact with Counsel</u>

During the month, I maintained regular contact with counsel for both parties.

II. <u>Eli-Weekly Status Reports</u>

I am enclosing the September 3 and 17,2002 United States' Status Reports that document the efforts undertaken by the Departments of the Interior and Treasury to comply with Paragraph 19 of the Court's November 27, 1996 First Order for Production of Information. See Exhibit 1. Of particular note and merit is the report of Ethel Abeita, Acting Director Office of Trust Records ("OTR') attached to the September 17,2002 bi-weekly report. Ms. Abeita's thoughtful analysis of the problems confronting the records management program is refreshing when compared to the offerings of OTR's previous directors.

III. <u>Conference with Acting Director – Office of Trust Records</u>

On September 10, 2002, Ms. Abeita conducted a briefing for Associate Deputy Secretary James Cason, Department of Justice Attorneys Sandra Spooner and Amalia Kessler, Assistant Deputy Secretary Abraham Haspel and myself. Also in attendance, in an advisory capacity, was former OTR Director Joe

Attachment **A**

Christie. Ms. Abeita briefed the attendees about OTR's workload, work plan, its efforts to define trust records and its efforts to identify the end users of trust records. See Exhibit 2.

IV. Department of the Interior Computer Systems

- Reconnection efforts remain underway for Interior's computer systems that were impacted by the Court's December 5,2001 Order. Interior officials have been working with Special Master contractor USinternetworking ("USi") to ensure that those systems that have already been reconnected or re-opened remain secure. **As** indicated in prior reports, the sensitivity of the information associated with those efforts preclude its inclusion in the monthly reports.

- In addition, USi has been working with SAIC to develop protocols to safely monitor the security of Interior's computer systems.

- On December 21,2001, Interior sought permission to reconnect its Minerals Management Service ("MMS") systems to the Internet. ***See*** December 2001 Monthly Report of the Special Master at (IV)(d). Based on USi's representations that reconnecting **MMS**' Denver, Colorado site to the Internet will not adversely impact individual Indian trust data residing on that system, on September 25,2002, I approved Interior's request to reconnect that site. *See* Exhibit **3.**

V. Investigation Relating to the Court's September 17,2002 Memorandum Opinion and Order

- On September 17,2002, the Court referred plaintiffs' October 19,2001 motion for order to show cause to the Special Master and ordered that a report and recommendation issue with respect to each of the 37 non-party individuals named in plaintiffs' motion. Order at 4 (September 17,2002). The Court simultaneously referred plaintiffs' March 20, 2002 motion for order to show cause why the alleged Interior contemnors and their counsel should not be held in contempt for destroying e-mail to the Special Master and ordered him to draft a report and recommendation on the issues raised therein. Id. In accordance with these orders, the Special Master has devised **a** set of protocols setting out each step of both investigations. These protocols will be distributed to all counsel within the next few days.

VI. Other Investigations

- In addition to the investigation into the issues raised by plaintiffs' October 19,2001 and March 20,2002 motions for orders to show cause, the Court directed me to investigate the allegations raised by Native American Industrial Distributors, Inc. in its August 29,2002 motion to intervene.

- My investigation into the IT practices of the Department of the Interior will conclude this month with the issuance **of** a final report.

VII. Reauest for Compensation

I am enclosing my request for compensation at market rates for services rendered and expenses incurred during the month of September 2002. My contemporaneous time records reflect the time consistent with the nature of my undertaking and the proper discharge of my responsibilities. Where appropriate, **I** have delegated responsibility to my associate, as indicated by her initials on my monthly bill. The amount of this month's invoice has been reduced by $530.24 because an internal audit **of** my past invoices revealed a duplicate photocopy charge in my June 2002 invoice. ***See*** Exhibit **4.**

I am also enclosing the invoice of Joe Christie for his continued assistance. See Exhibit 5.

Finally, I am enclosing the bill of IBM Global Services for work performed regarding DOI computer systems for the period beginning June 15, 2002 and ending July 12,2002, and the August and September 2002 bills of USi for services rendered in monitoring and analyzing the security of Interior's computer systems. ***See*** Exhibit **6.**

Respectfully submitted,

Alan L. Balaran

cc: Dennis M. Gingold, **Esq.** (w/attachments)
Sandra Spooner, **Esq.** (w/attachments)

LAW OFFICE

ALAN L. BALARAN, P.L.L.C.

ADMITTED IN DC AND MD

1717 PENNSYLVANIA AVE., N.W.
TWELFTH FLOOR
WASHINGTON.D.C. 20006
TELEPHONE (202) 466-5010
FAX (202) 986-8477
E-MAIL abalaran@erols.com

February 3,2003

Honorable Royce C. Lamberth
United States District Court
for the District of Columbia
333 Constitution Ave., N.W.
Washington, D.C. 20001

RE: **Cobell et al. v. Norton et al., C.A. No. 96-1285**
January 2003 Report of Special Master

Dear Judge Lamberth:

In accordance with this Court's Order dated February **24,** 1999 appointing me **as** Special Master, **I** am submitting my report regarding matters presented to me during the month of January 2003.

I. Contact with Counsel

During the month, I maintained regular contact with counsel for both parties.

II. Bi-Weeklv Status Reports

I am enclosing the January **7** and 21,2003 United States' Status Reports that document the efforts undertaken by the Departments of the Interior **and** Treasury to comply **with** Paragraph 19 of the Court's November 27, 1996 First Order for Production of Information. ***See*** Exhibit 1.

III. Department of the Interior Comuuter Systems

- Reconnection efforts remain underway for the Department of the Interior's ("Interior") computer systems that were impacted by the Court's December 5, 2001 Order. Interior officials have been working with Special Master contractor US internetworking ("USi") to ensure that those systems that have already been reconnected or reopened remain secure. Given the sensitivity of the information associated with those efforts, USi's site visit reports will not be attached hereto but have been transmitted to counsel under separate cover.

- During the month, I convened weekly information technology meetings with USi; Interior officials; representatives from the Department of Justice and SAIC, Interior's contractor. The Special Master and Intenor have agreed, in principle, to "rules of engagement" that would govern USi's scans of Interior computer systems. Once a final copy is promulgated, it will be distributed to the Court and parties.

- During the month **I** provided counsel with USi's assessments of the security of the BIA systems located in Wewoka and **Ada,** Oklahoma and USi's assessment of the current connectivity of BIA's Land Title Mapper system, located in Lakewood, Colorado. USi's site visit to the Wewoka agency revealed that a file server was accessing the Internet without prior authorization. This server has been since been shut down and an investigation begun to determine responsibility for the unauthorized reconnection.

- To ensure that security problems identified by IBM or USi have been addressed, on January 15,2003, **I** requested that each **of** Interior's Bureau Chief Information **Officers** detail, in writing all remedial steps taken to date.

IV <u>Investigation Relating to tl Court's **September** 17,2002 4(Opinion and Order</u>

- **During** the past month, individuals named in plaintiffs' March 20,2002 Motion for Order to Show Cause Why Interior Alleged Contemnors **and** Their Counsel Should Not Be Held in Contempt for Destroying E-mail, filed briefs seeking dismissal of the Bills **of** Particulars filed against them. The deadline for plaintiffs to respond **is** February **17,2003.**

V. <u>Investigation into the Destruction **of E-Mail** Messages</u>

- On January 27,2003, **I** issued my report and recommendation concerning **the** deletion **of** e-mails by former Assistant Secretary-Indian Affairs Neal McCaleb.

VI. Miscellaneous

- On January 15,2003, I issued my opinion regarding plaintiffs' application for fees and expenses incurred in connection with the prosecution of allegations lodged by BIA employee Mona Infield. Given the complexity of the issues presented, I retained the services of Michael Gaffney, Gaffney & Schember, P.C., a recognized expert in the field of fee petitions. I am enclosing the December 2002 invoice of Michael Gaffney, for his assistance in drafting the SO-page fee opinion. (Mr. Gaffney's January 2003 invoice will be attached to the next monthly report of the Special Master.) See Exhibit 2. To minimize costs, Mr. Gaffney agreed to substantially discount his hourly fee and I have not billed for my time spent working with Mr. Gaffney on the report.

- During the month, I received information concerning the unauthorized use of a password at the Crow Creek Agency. I directed the Acting Director of the Great Plains Region to forward whatever information she had concerning this incident. Once I have reviewed this information, I will make my findings known to the Court and parties.

- On October 7,2002, I requested that Interior provide me with documents relating to my investigation into allegations made by Native American Industrial Distributors. I clarified that request on January 29,2003; on January 31,2003, Interior agreed to provide me with all requested documents by February 14,2003. See Exhibit 3.

- On September 25,2002, the Special Master issued an opinion (filed on January 17, 2003), approving Interior's request to contract with Zantaz to electronically capture, archive and search Interior's e-mail transmissions. On January 24,2003, Interior forwarded a current status report outlining Zantaz' efforts, including those undertaken to retrieve communications deleted by former Assistant Secretary Neal McCaleb. See Exhibit 4.

- On January 31,2003, the Special Master visited the OIRM facility in Reston, Virginia to report on the security measures in place at the facility and the impact of those measures on the safety of IIM trust data. The Special Master will issue the results of that site visit in the next few days.

- During my investigation into the deletion of electronic messages by former Assistant Secretary Neal McCaleb, it came to light that Interior employees were using home computers to transmit work-related information. The Special Master requested that Interior issue a directive prohibiting such activity pending a formal inquiry to determine the extent to which individual Indian trust information was transmitted along insecure internet lines. By memorandum dated January 30,2003, Interior Deputy Secretary J. Steven Griles directed Interior employees to house, process or store individual Indian trust data only on "properly configured DOI computer[s]" and transmit such information only on "DOI configured virtual private networks." See Exhibit 5.

VII. Request for Compensation

I am enclosing my request for compensation at market rates for services rendered and expenses incurred during the month of January 2003. My contemporaneous records reflect time consistent with the nature of my undertaking and the proper discharge of my responsibilities. Where appropriate, I have delegated responsibility to my associate, as indicated by her initials on my monthly bill. This month's invoice has been reduced by $80.00 to reflect an overpayment to my January 2003 invoice. *See* Exhibit 6.

I am also enclosing the January 2003 invoice of USi for services rendered in monitoring and analyzing the security of Interior's computer systems. *See* Exhibit 7.

Respectfully submitted,

Alan L. Balaran

cc: Dennis M. Gingold, Esq. (w/attachments)
Sandra Spooner, Esq. (w/attachments)

U.S. Department of Justice

Civil Division, Commercial Branch
1100 L Street, N.W., Room 10030
Washington, D.C. 20005

John Warshawsky *Telephone: (202) 307-0010 Facsimile: (202) 514-9163*

November 22,2002

By Facsimile

Mr. Alan Balaran, Special Master
1717 Pennsylvania Avenue, N.W.
Twelfth Floor
Washington, D.C. 20006

Re: Cobell v. Norton – Rules of Engagement for Testing by USinternetworking, Inc. (Network Discovery, Vulerability/Penetration Testing, and Exploitation Limits Testing)

Dear Mr. Balaran:

In accordance with our discussion on November 14,2002, attached please find the Interior Department's proposal for Rules of Engagement for the testing to be conducted by USi. Please advise me whether you have any questions or comments regarding this proposal.

Thank you, again, for your efforts with regard to the preparation of this protocol for testing.

Very truly yours,

John Warshawsky
Trial Attorney
Commercial Litigation Branch
Civil Division

cc: Mr. Dennis Gingold (by facsimile)
Mr. Keith Harper (by facsimile)

Attachment C

Rules of Engagement for Testing on Behalf of Special Master bv USinternetworking, Inc.

Overview

The following Rules of Engagement ("ROE") provide the framework for procedures to be followed with respect to information technology ("IT") testing to be performed on behalf of the Special Master in Cobell v. Norton, Case No. 1:96CV01285 (D.D.C.) (pending), with regard to the Interior Department's ("DOI") IT infrastructure. These tests will be performed by the Special Master's expert, USinternetworking, Inc., ("USi") and are referred to herein as "USi's Testing."

USi's Testing will consist of the following four phases, which are identified and described on the attached USi document, entitled "USi Methodology for DOI Network Discovery and Penetration Testing":

- Phase One: Open-Source Information Gathering
- Phase Two: Network Asset Discovery
- Phase Three: Vulnerability/Penetration Testing
- Phase Four: Exploitation Limits Testing

USi will conduct its tests in accordance with the terms of these ROE.

Objectives of USi's Testing

USi's Testing will attempt to identify and expose vulnerabilities in DOI's IT infrastructure to evaluate whether systems that house or provide access to Individual Indian Trust Data ("IITD") are vulnerable to unauthorized access and use. Consistent with industry best practice, USi will conduct its testing in a manner designed (a) to minimize operational impact impact by using techniques that will not deliberately disable users or deny service, (b) to safeguard any data accessed by using methods that wilt not intentionally modify or change any data accessed, and (c) to prevent and, if necessary, to permit expeditious remediation of any damage to DOI's IT systems or data resulting from USi's Testing.

USi's Testing is not intended to assess National Critical Infrastructure Systems, i.e., Supervisory Control and Data Acquisition systems located at the Hoover Dam, Grand Coulee Dam, and Shasta Dam. In the event additional additional systems are designated as National Critical Infrastructure Systems, DOI will notify the Special Master of such designation, through Justice Department counsel, and those systems will not be subject to USi's Testing.

Procedures to Minimize Oaerational Impact and to Protect Svstems and Data

USi's Testing will comply with the procedures described below to minimize operational impact and to prevent damages and, if necessary, to permit expeditious remediation of any damage to DOI's IT systems **or** data resulting from USi's Testing:

Documentation and Reporting

USi will maintain documentation of all actions taken in the course of its testing. Such documentation shall be sufficient to enable a reviewing party to reconstruct systems tested, steps taken, tools utilized, and tool settings employed by USi. **As** a minimum, the documentation shall include the following:

- Test Plans for each targeted system;
- **A** journal documenting activities and times during the testing, a **copy** of which will be included with the monthly report discussed in the section below entitled "Periodic Reporting by USi";
- Output of **a** scripting tool used to capture **all** manual command-line testing efforts, a copy of which will be included with the monthly report discussed in the section below entitled "Periodic Reporting **by** USi"; and
- **A** Tool List containing all open-sourced **and** commercial scanning and assessment tools with version numbers.

Trusted Points-of-Contact

DOI recognizes the interest of the Special Master to maintain the confidentiality of the testing **to be** undertaken by USi, and the Special Master recognizes **DOI's** interest in protecting **its** systems and data from damage resulting from such testing. **In** light of the foregoing interests, **DOT** designates the following Trusted Poinls-of-Contact ("TPOC"):

(1) DOI TPOCs:

- Roger Mahach, DOI IT Security Manager, **and** one or more subordinates of Mahach, who **will** be identified to the Special Master **and** USi **in** advance of their performing **any** duties as DOI TPOC.
- James Cason, DOI Associate Deputy Secretary, and Judy Snoich, DOT Project Office, and one or more additional subordinates **of** Cason, who will **be** identified to the Special Master and USi in advance of their performing any duties as DOI TPOC.

(2) SAIC TPOCs: Hart Rossman and Jon Pettyjohn, employees of DOI's expert, **SAIC.**

(3) Incident-Response TPOC: One or more employees or contractors of the Federal Computer Incident Response Center ("FedCIRC") or other incident-response contractors, who will be identified to the Special Master and USi in advance of their performing any duties as TPOCs.

(4) Government Counsel TPOC: John Warshawsky and Glenn Gillett, U S. Department of Justice, and other attorneys employed **by** the United States in conjunction with **the** Cobell litigation, who **will** be identified to **the** Special Master and USi in advance of their performing any duties as TPOCs.

All TPOCs will review a copy of these ROE and will execute an acknowledgment form confirming their understanding of the ROE and the restrictions described in the paragraph below, which **are** placed upon them by the ROE.

The DOI TPOCs, **SAIC** TPOCs, and Government Counsel TPOCs will be provided advance notice by USi of Test Plans for Phases Two, Three, and **Four.** The contents of the Test Plans are described in the section below, entitled "Test Plans." These TPOCs will not disclose any details of the Test Plans to anyone other than another TPOC, except for the following:

(1) The DOI TPOCs may disclose such information to the Incident-Response TPOC for purposes of identifying USi's Testing efforts in the course of normal incident-reporting procedures, and

(2) The TPOCs **may** disclose information to non-TPOCs in the event such notice becomes necessary (a) to minimize operational impact, (b) to prevent or remediate any damage **to** DOI's IT systems or data resulting from USi's Testing, or (c) to respond to an unsolicited inquiry from **a** non-TPOC regarding any suspicious activity identified in the course of routine systems monitoring activities.

The TPOCs shall notify the Special Master promptly of the disclosure of any information to **a** non-TPOC. **Such** notification shall be made through Justice Department counsel.

Test Plans

Phase One: Prior to commencing Phase One Testing, USi will provide the DOI TPOCs, SAIC TPOCs, and Government Counsel TPOCs a Test Plan, in writing, which will identify the target of its information-gathering activities.

Phase Two: Prior to commcncing Phase Two Testing, USi will provide the DOI TPOCs, SAIC TPOCs, and Government Counsel TPOCs a Test Plan, in writing, which will list the targeted systems and IP address ranges identified during the information-gathering activities in Phase One,

Phase Three and Phasc Four: Prior to commencing any Phase Three or Phase Four Testing, USi will provide to thc DOI TPOCs, **SATC TPOCs,** and Government Counsel TPOCs a Test Plan, in writing, which will include, as a minimum, the following:

- Description of the testing to be performed, including whether the test shall be internal or external to DOI's IT infrastructure and whether the testing shall be done remotely or locally;

a The category of system abuser that will be simulated by USi's test, i.e., (a) an outsider without knowledge about **DOI's IT** environment, (b) an outsider with knowledgc about DOI's IT environment, (c) **an** insider without knowledge about DOI's IT environment, and/or **(d)** an insider with knowledge about DOI's IT environment rcsources;

- Description of tools, techniques, and methodology to be utilized;

- IP Address ranges of the hosts from which the testing **shall** be conductcd or launched;

- IP address ranges to be targeted and tested; and

- Anticipated duration for the testing.

Upon receipt of a Test Plan for Phasc Three or Phase Four, the TPOCs will promptly review it to ascertain whether thc proposed testing will or may (a) cause operational impact to a mission-critical system or (b) compromise or damage the integrity of any data on a system. DOI's TPOC will advise USi, in writing, within five (5) business days of any such concerns and any proposals for modification of thc Test Plan. USi will have the discretion to accept or reject any proposed modifications, **and** USi shall notify DOI's TPOC of any such decision, in writing, no less than three **(3)** days before proceeding with its testing. In the event DOI's TPOC dccms it necessary to protect its systcms or data, DOI reserves the right to contact thc Special Master, through an appropriate TPOC, during the period prior **to** USi's commencing its testing, to seek appropriate rclicf.

Implementation of Test Plans

Throughout the Phase Three and Phase Four testing, **DOT** will have the opportunity to observe USi's staff conducting the testing and to provide any further coordination deemed necessary to protect systems or data from permanent damage. In the event a test procedures causes unexpected results resulting **in** a negative impact to a system (e.g., denial of service; alteration, modification, or deletion of files or file-structure; system crash; or system **fails** in an "open" state), DOI shall be permitted to undertake **any** necessary **steps** to prevent further damage and to effect recovery.

Periodic Reporting by USi

USi **will** prepare a summary of its testing activities on a monthly basis, describing systems subjected to its testing procedures during the preceding month, steps performed with regard **to** the systems, and any findings regarding vulnerabilities. USi will provide **a copy** of **its monthly** summary **to** Justice Department counsel, **who** will provide copies to DO1 **TPOCs, SAIC** TPOCs, and Government Counsel **TPOCs.** In addition, USi will make its documentation available to the DOI TPOCs, SAIC TPOCs, and Government Counsel TPOCs upon their rcqucst.

Securitv Clearances

Because of **the** sensitive nature of information **that** may **be** reviewed and collected during the course of USi's Testing, **all** USi employees engaged in the performance of its test procedures shall possess, as a minimum, an active and current Secret National Security clearance.

USi

USinternetworking, Inc.™

USi Methodoiogy for DOI Network Discovery and Penetration Testing

This methodology describes the high level details of the steps used to discover, assess, and test Department of Interior (DOI) network assets accessible from the Internet, with an aim towards identifying unprotected Indian Trust Data (ITD). The primary target of these tests includes those agencies that fall under the Temporary Restraining Order (TRO) yet still maintain an Internet presence.

The testing is divided into four distinct categories: open-source information gathering, network asset discovery, vulnerability/penetration testing, and exploitation limits testing. DOI agencies will be tested consecutively according to a time schedule. These categories of testing typically *are* conducted in the order listed. Concurrently, monitoring for active hosts within IP address ranges restricted by the TRO will be conducted, and any discoveries logged. Active IP addresses detected within restricted ranges will be included in additional vulnerability/penetration testing.

Description of the four testing categories...

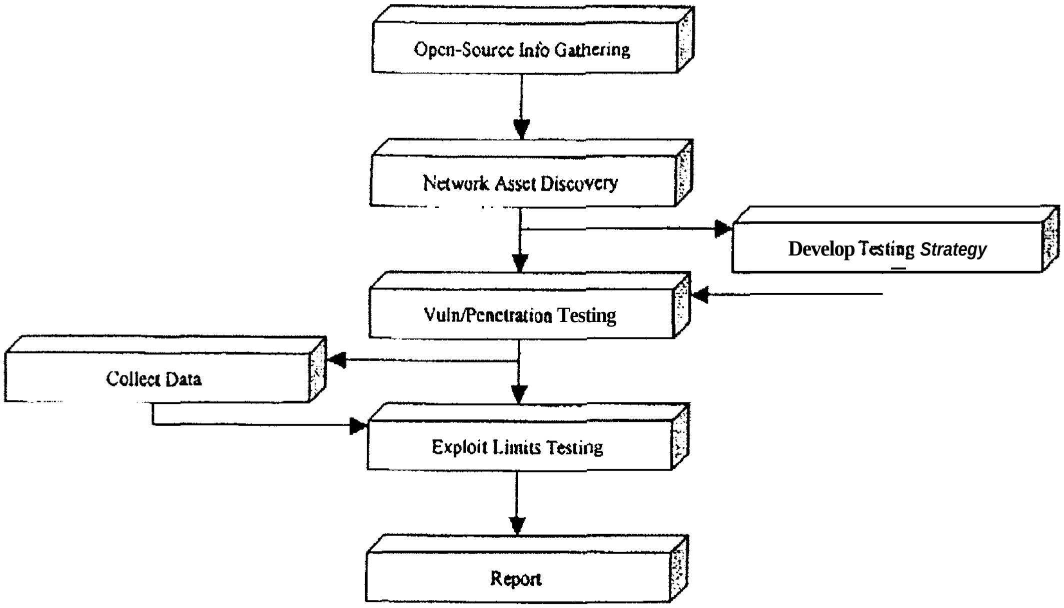
1. *Open-source information* gathering: Includes searching of publicly accessible web sites related *to* or run by the DOI agencies, as well as other public Internet information repositories. This testing does not include any exploitation of vulnerabilities, merely the gathering of infomation available with minimal effort. Social engineering techniques may be employed.

2. *Network Asset Discovery:* Includes efforts to identify active hosts and network devices, the services that they may be offering, and network topology. This information is gathered primarily as a precursor for vulnerability/penetration testing and used to develop an effective testing strategy.

3. *Vulnerability/Penetration Testing:* Tools and utilities are used to gather further information concerning DOI agency hosts and network devices, Common exploitation techniques are used, and configurations problems are identified. Stealthy exploitation/assessment techniques are used.

4. ***Exploitation Limits** Testing*: Determines the extent of which a **network** can be further penetrated using systems that have been exploited. Links and traces to other systems or networks are tested, and further information gathering is conducted.

The following diagram depicts the typical **progression** of **a** network discovery and penetration test...



Detailed Tool Usage Methodology

This scction describes the specific tactics and tools used to perform the assessment. These procedures form the foundation of the testing, however additional testing may bc warranted under certain circumstances.

Open-Source Info Gathering

The testers will use open-source Internet resources to gather information about the target. These sources often include Internet WIIOIS databases, DNS records, search engine queries, public Web sites, and Usenet newsgroups. The goal is to gather as much information as possible without actually having to connect to the target's networks (with the exception of'accessing the target's public Web sites). The additional information gathered will allow more specific follow-up testing.

Examples of tools used during this step: web browscrs (i.e. Internet Explorer, Lynx, Netscape), WHOIS database servers, DNS server query tools (i.e. nslookup, DIG), and Uscnct clicnts (i.c. Outlook Express).

Network Asset Discovery

This step is simcd at identifying the individual hosts, routers, and network devices that are publicly accessible from the Internet. The typical methodology is to use port scanner.; and network route tracing. Most of these methods attempt to use stealth technology to prevent detection by the target network. Hence, many of these procedures can span long periods of time. The information gathered during these proccdurcs will be used to formulate a more specific target strategy in the following steps.

Examplcs of tools used during this step: NMAP, traceroutc, and SuperScan.

Vulnerabilitv/Penetration Testing

Once the preliminary data has been gathered, actually vulnerability testing begins using a variety of testing tools. These toots attempt to identify actual vulnerabilities by using commonly known attack techniques for the many flavors of vulncrabilities that exist. In the case of vulnerabilities that do not endanger the system (such as denial-of-service attacks), the vulnerabilitics will be exploited to determine the validity of the problem. Automated scanners that test many different targets in a short duration are used during this step.

Examples of tools used during this step: Nessus, Whisker, AMAP, Retina SQL Scanner, SQL Dict, and SNMPGET/SNMPWALK.

Exploitation Limits Testing

Once vulnerabilities are discovered additional testing is conducted to determine the extent to which a system can be exploited. Oftentimes a vulnerable host will be used as a "middle-man" to attack other systems in thc surrounding networks. This phase of the assessment involves testing the limits of how far a network can be exploited. This testing will usually involve gaining access directly on the target systems.

Examples of tools used during this step: PCAnywhere, Terminal Services, RDP Desktop, and VNC

NMAP (Unix: TCP/UDP port scanner and host discovery tool)
This tool is used to identify available TCP and UDP services on hosts, as well as identify live hosts within u specified IP range.

Nessus (Unix: vulnerability assessment tool)
This tool scans multiple hosts for known vulnerabilitics such as buffer overflows, weak passwords, and many others. Nessus will always bc configured NOT to do any denial-of-service attacks

Whisker (Unix: Web CGI vulnerability Scanner tool)
This tool will test a Web server for known CGI exploits and gather rcsponsc data from the server.

AMAP (Unix: TCP service identification and query tool)
This tool uses the output from an NMAP scan and tests open TCP services to determine the type of application running. For example, it will identify an SSH service running on a non-standard SSH port.

SuperScan (Windows: TCP/UDP port scanner and host discovery tool)
This tool is similar to the NMAP tool. However, it runs from Windows instead of Unix.

SQL Dict (Windows: MS SQL brute-force password guessing tool)
This tool attempts to brute-force guess MS SQL accounts and passwords that are weakly configured. An example of what it may find includes an "sa" account with a blank or "sa" password.

Retina SQL Scanner (Windows: MS SQL vulnerability scanner tool)
This tool scans multiple hosts looking for MS SQL servers that are vulnerable to the latest exploits and worms.

SNMPCET and SNMPWALK (Unix: SNMP service querying tools)
These tools query an SNMP service to gather information such as network settings and in some cases user accounts.

Trrceroute (Unix and Windows: networking path discovery tool)
This tool comcs standard with many Unix and Windows operating systems, and allows the network path from one system to another to be traced. The output shows what routers or gateways lie between the two systcms.

PCAnywhere Client (Windows: remote access tool)
This tool is used to connect to PC Anywhere services to gain remote console access to the host.

Terminal Serviccs Client (Windows: remote access tool)
This tool is used to connect to Terminal Services on Windows machines to gain remote terminal access to the hosts.

VNC Client (Unix and Windows: remote access tool)
This tooi is used io connect to VNC serviccs on Windows or Unix systems to gain remote console access to the hosts.

RDP Desktop (Unix: Terminal Services clicnt remote access tool)
This is the Unix equivalent to the Windows Terminal Services client.

SMB Tools (SMBCLIENT, NMBLOOKUP)

```
*************** -COMM. JOURNAL- ****************** DATE NOV-22-2002 ***** TIME 13:18 ********

     MODE = MEMORY TRANSMISSION              START-NOV-22 13:07     END=NOV-22 13:18

       FILE NO.=996

STN   COMM.     ONE-TOUCH/   STATION NAME/TEL NO.                       PAGES     DURATION
NO.             ABBR NO.

001   OK        *            99868477                                   012/012   00:02:54
002   OK        *            93182372                                   012/012   00:03:42
003   OK        *            98220068                                   012/012   00:02:12


                                                  -DOJ/CIVIL DIVISION       -

************************************* -           - ***** -        202 514 9163- *********
```

FACSIMILE TRANSMITTAL

To:

Mr. Alan L. Balaran [Facsimile number (202) 986-8477]
Mr, Dennis M. Gingold [Facsimile number (202) 318-2372]
Mr. Keith Harper [Facsimile number (202) 822-0068]

From:

John Warshawsky, Trial Attorney
United States Department of Justice
Commercial Litigation Branch, Civil Division
1100 L Street, N.W., Room 10030
Washington D.C. 20005

Office telephone: (202) 307-0010
Facsimile number: (202) 514-9163

Pages (including cover page): 12

Comments:

Date of transmission: Friday, November 22, 2002

NOTE THIS FACSIMILE IS INTENDED ONLY FOR THE ABOVE-DESIGNATED ADDRESSEE. IT MAY CONTAIN INFORMATION WHICH IS PRIVILEGED, CONFIDENTIAL, OR OTHERWISE PROTECTED FROM DISCLOSURE TO ANYONE OTHER THAN THE ADDRESSEE

IF YOU ARE NOT THE ADDRESSEE AND HAVE RECEIVED THIS FACSIMILE IN ERROR

(1) PLEASE DO NOT REVIEW, DISSEMINATE, OR OTHERWISE USE ANY OF THE TRANSMISSION, AND

(2) PLEASE ADVISE THE SENDER OF THIS FACSIMILE IMMEDIATELY

United States Department of Justice
Civil Division
Commercial Litigation Branch

SANDRA P. SPOONER
DEPUTY DIRECTOR

P.O. BOX 875, BEN FRANKLIN STATION
WASHINGTON, D.C. 20044-0875

TEL: (202) 514-7194
FAX: (202) 307-0494
EMAIL: SANDRA.SPOONER@USDOJ.GOV

December 21,200I

__Bv Facsimile__

Alan L. Balaran, Esq.
1717 Pennsylvania Avenue, N.W.
12th Floor
Washington, D.C. 20006

Re: Cobell v. Norton - Notice of Intention to Reconnect to the Internet All Office of Surface Mining Information Technology Systems

Dear Mr. Balaran:

The Consent Order entered by the Court on December 17,2001, contains the following provision:

> ORDERED that Interior Defendants may reconnect to the Internet any information technology system that does not house individual Indian trust data and that does not provide access to individual Indian trust data seventy-two (72) hours after providing actual notice with appropriate documentation to the Special Master and Plaintiffs counsel or immediately upon concurrence of the Special Master. . . .

I am writing to provide notice and appropriate documentation regarding the Department of the Interior's intention to reconnect the Office of Surface Mining (OSM) to the Internet. The enclosed statement of Glenda Owens, Acting Director, OSM, documents that OSM's applications systems, servers and workstations do not house or provide access to individual Indian trust data. This statement is made on the basis of reasonable inquiry and the following information. **As** further verification, we sought confirmation from the Bureau of Indian Affairs that the lack of individual Indian trust data in OSM systems was consistent with BIA's expectations. The statement of James. H. McDivitt, Deputy Assistant Secretary – Indian Affairs is enclosed.

OSM has obtained certifications concerning the content of each of its approximately 1300 IT systems. Individuals knowledgeable about the intended purposes of the databases contained

Attachment D

within each system certified, with the one exception set out below, that, to the best of their individual knowledge and belief, the system did not contain Indian trust data. Because there is no practical **way,** given the substantial volumes of information stored in some systems, to evaluate every document or data set stored in each database individually, the certifications are based upon a standard **of** reasonableness. Nevertheless, the certification process did include instructions for searching for such information. The certifications are stored in the office of Roy Morrison, Team Leader, Network Systems Support Team, Division of Information Systems Management, OSM, 1951 Constitution Avenue, **N.W.,** Washington, D.C. **20240, (202) 208-**2810.

The one exception cited above was identified **as** potentially relevant **as** a result of the search made for data **in** the **OSM** IT systems. **A** copy of the document is enclosed, but is no longer accessible by **OSM** IT systems because it has been downloaded to a compact disk and put in a secure location.

Prior to the temporary restraining order, OSM provided communications support for the Solicitor's Office. The Solicitor's Office manages **a** wide variety of legal issues and, as a result, has been unable to certify that its information technology systems do not include individual Indian trust data. Therefore, **OSM** has severed the Solicitor's Office connections to its network until certifications **are** forthcoming (at which point, we propose to reestablish their communications connection) or other arrangements, acceptable to the Associate Deputy Secretary and the Special Master, are made.

Finally, enclosed is a schematic and verbal description of OSM's communications network and security system, and a list of contact information of key **OSM** personnel to assist you in the event you need additional information.

Under the circumstances, described here, the Consent Order permits reconnection to the Internet **72** hours after this notice and documentation is provided to you. Please let **us** know if this time is insufficient for your review.

Thank you for your consideration of this matter.

Sincerely,

Sandra P Spooner

SANDRA P. SPOONER

cc: Dennis Gingold (By FAX)
Keith Harper (By FAX)

United States Department of Justice
Civil Division
Commercial Litigation Branch

Sandra P. Spooner
Deputy Director

P.O. Box 875, Ben Franklin Station
Washington, D.C.20044-0875

Tel: (202) 514-7194
Fax: (202) 307-0494
Email.sandraspooncrOusdoj.gov

January 22,2002

Mr. **Alan** Balaran, Esq.
1717 Pennsylvania Ave., NW
12th Floor
Washington, DC 20006

Re: Cobell v. Norton -Recommencement of OSM Systems

Dear Mr. Balaran:

My letter earlier today regarding the Office of Surface Mining was imprecise. You advised that OSM could, **as** proposed in its letter **of** December 21,2001, reconnect its IT systems to the Internet. We appreciate your consideration of this matter.

Sincerely,

SANDRA P. SPOONER

cc: Dennis Gingold (by FLY)
Keith Harper (by FAX)

Attachment E

CERTIFICATE OF SERVICE

I declare under penalty of perjury that, on June 27,2003 I served the foregoing *Interior Defendants' Opposition to Plaintiffs' Consolidated Motion for a Temporary Restraining Order and Motion for a Preliminary Injunction to Ensure the Protection of Individual Indian Trust Data* by facsimile in accordance with their written request of October 31, 2001 upon:

Keith Harper, Esq.
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 822-0068

Dennis M Gingold, Esq.
Mark Kester Brown, Esq.
607 - 14th Street, NW
Box **6**
Washington, D.C. 20005
(202) 318-2372

Per the Court's Order of April 17,2003,
by facsimile and by U.S. Mail upon:

Earl Old Person *(Prose)*
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
(406) 338-7530

By U.S. Mail upon:

Elliott Levitas, **Esq**
1100 Peachtree Street, Suite 2800
Atlanta, **GA** 30309-4530

By facsimile and U.S. Mail:

Alan L. Balaran, Esq.
Special Master
1717 Pennsylvania Avenue, N.W.
13th Floor
Washington, D.C. 20006
(202) 986-8477

K. P. Kingston
Kevin P. Kingston